CLAIMS:

1. A microelectronic circuit arrangement (100) intended for protecting at least one electronic component (200) against illicit manipulation and/or unauthorized access, having at least one activating unit (Ai; i = 1, 2, 3, 4, 5) for checking that at least one activating condition is met and for activating at least one preventing unit (Vj; j = 1, 2, 3, 4, 5, 6, 7) that is also associated with the circuit arrangement (100) and that is connected to the activating unit (Ai), by means of which preventing unit (Vj) the component (200) can be at least partly de-activated and/or at least partly destroyed in the event of illicit manipulation and/or unauthorized access.

2. A circuit arrangement as claimed in claim 1, characterized in that the preventing unit (Vj) is constructed

- in analog circuit technology or
- in at least directly digital circuit technology, in the form of for example at least one fuse and/or at least one antifuse.

3. A circuit arrangement as claimed in claim 1 or 2, characterized in that the activating unit (Ai) is arranged

(i = 1) to recognize once or more than once at least one illicit command,

(i = 2) to recognize a multiplicity of different illicit operations,

(i = 3) to issue at least one specific activating command

(i = 4) to issue at least one activating command together with data that addresses a plurality of components by means of at least one group coding, or an individually coded component, and/or

(i = 5) to recognize once or more than once at least one physical attack on the component (200), by means of sensor circuitry belonging to the component (200) that is intended for this purpose.

4. A circuit arrangement as claimed in any of claims 1 to 3, characterized in that the preventing unit (Vj) is arranged

(j = 1) to prevent an internal oscillator from beginning to oscillate

(j = 2) to prevent an oscillator for an external clock signal from beginning to oscillate,

(j = 3) to switch off a high-voltage limiter, in particular by means of permanent programming,

(j = 4) to prevent the build-up of a high voltage,

(j = 5) to reprogram the allocation of addresses and/or the allocation of data,

(j = 6) to load the memory element (210) of the component (200) with illicit values of data, and/or

(j = 7) to switch on an increased current drain in the operating state or the quiescent state.

5. A method of protecting at least one electronic component (200) against illicit manipulation and/or unauthorized access, characterized by the following method steps:

(i) checking that at least one activating condition is met by means of at least one activating unit (Ai, i = 1 2, 3, 4, 5),

(ii) in the event of illicit manipulation of the component (200) and/or unauthorized access to the component (200): activating at least one preventing unit (Vj; j = 1, 2, 3, 4, 5, 6, 7) that is connected to the activating unit (Ai), and

(iii) at least partly de-activating the operation of the component (200) and/or at least partly destroying the component (200), by means of the preventing unit (Vj).

6. A method as claimed in claim 5, characterized in the check on whether the activating condition is met is made

- by analyzing at least one data stream applied from outside or
- by signals from the internal sensor circuitry of the component (200).

7. A method as claimed in claim 5 or 6, characterized in that, if the activation condition is met

- recognition of this fact (A1, A2, A3, A4, A5) and the desired effects it is to have (V1, V2, V3, V4, V5, V6, V7) are placed in store in coded form in at least one memory element (210) that is used for starting-up the component (200), and
- the start-up, which initiates the appropriate actions, is repeated.

8. A method as claimed in any of claims 5 to 7, characterized in that the activation takes place

(i = 1) as a result of the recognition once or more than once of at least one illicit command,

(i = 2) as a result of the recognition of a multiplicity of different illicit operations,

(i = 3) as a result of the issue of at least one specific activating command,

(i = 4) as a result of the issue of at least one activating command together with data that addresses a plurality of components by means of at least one group coding, or an individually coded component, and/or

(i = 5) as a result of the recognition once or more than once of at least one physical attack on the component (200), by means of sensor circuitry belonging to the component (200) that is intended for this purpose.

9. A method as claimed in any of claims 5 to 8, characterized in that the at least partial de-activation of the operation of the component (200) and/or the at least partial destruction of the component (200) is carried out by

(j = 1) preventing an internal oscillator from beginning to oscillate,

(j = 2) preventing an oscillator for an external clock signal from beginning to oscillate,

(j = 3) switching off a high-voltage limiter, in particular by means of permanent programming,

(j = 4) preventing the build-up of a high voltage,

(j = 5) reprogramming the allocation of addresses and/or the allocation of data,

(j = 6) loading at least one memory element (210) of the component (200) with illicit values of data, and/or

(j = 7) switching on an increased current drain in the operating state or the quiescent state.

10. Use of at least one circuit arrangement (100) as claimed in any of claims 1 to 4 and/or of the method as claimed in any of claims 5 to 9 for the self-destruction of at least one integrated circuit in the event of unauthorized use in the field or of an illicit attempt to analyze the integrated circuit by at least partial reverse preparation.